IN THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1.   (Currently Amended) A method of processing data, the method comprising:
        receiving data from a network link;
        replicating said data on board a network analyser card to produce at least two <u>new replica</u> editions of <u>one or more frames of</u> the received data; and
        writing said <u>at least two new replica</u> editions of the received data to an area of memory in a host that is directly accessible by a host application.

2.   (Previously Presented) The method according to claim 1, comprising:
        processing said editions of data stored in the said area of memory accessible by a host application, the processing comprising executing a different set of rules relating to intrusion detection on each edition.

3.   (Previously Presented) The method according to claim 1, in which the data is replicated using hardware.

4.   (Previously Presented) The method according to claim 1, in which the editions of the received data are provided as independent data streams.

5.   (Previously Presented) The method according to claim 1, in which each of the at least two editions of said received data is buffered independently.

6.   (Previously Presented) The method according to claim 4, in which each of the independent data streams is filtered according to desired criteria.

7.   (Previously Presented) The method according to claim 4, in which different filtering rules are applied to each of the editions of the received data.

8.   (Previously Presented) The method according to claim 1, the method comprising:

2

writing the editions of the received data to an area of kernel memory of the host memory; and

providing to the host application an offset to enable location of the data by the host application in the kernel space of the memory.

9.   (Previously Presented) The method according to claim 8, in which when data is written to the kernel space of the host memory a list of offsets with respect to a base address within kernel space is generated, the list of offsets serving to enable location of data packets within the kernel space with respect to the base address.

10.   (Previously Presented) The method according to claim 9, comprising:

providing to an application for running in application space, an offset to enable location of the base address of the data within the kernel space.

11.   (Previously Presented) The method according to claim 9, comprising:

providing to the application a list of offsets with respect to the offset of the base address.

12.   (Previously Presented) The method according to claim 1, in which the data is received as data frames from a network link.

13.   (Previously Presented) The method according to claim 12, comprising:

adding to substantially each of the received data frames a descriptor, the descriptor containing data relating to the data frame to which it is attached.

14.   (Currently Amended) A network analyser card for connection to a host and a network, the card comprising:

a receiver for receiving plural data frames from a network link;

data replication means for generating from the received data frames at least two new replica editions of one or more frames of the received data frames; and

a descriptor adder configured and arranged to add a descriptor to substantially each of the data frames of each of the at least two new replica editions of the received data frames,

3

the descriptor including data about the data frame to which it is attached for use in processing of the data frame.

15.   (Previously Presented) The network analyser card according to claim 14, comprising:

data writing means for writing the at least two replica editions of the received data frames to an area of host memory directly accessible by a host application.

16.   (Previously Presented) The network analyser card according to claim 14, in which the descriptor includes data indicative of the length of a data frame to which it is attached.

17.   (Previously Presented) The network analyser card according to claim 14, in which the descriptor includes a timestamp indicative of the time at which the corresponding data frame was received at the network analyser card.

18.   (Previously Presented) The network analyser card according to claim 14, wherein one or more of the data replication means, the descriptor adder and the data writing means is or are arranged in hardware.

19.   (Previously Presented) The network analyser card according to claim 14, the network analyzer card being controllable to execute the steps of:

receiving data from a network link;

replicating said data on board a network analyser card to produce at least two editions of the received data; and

writing said editions of the received data to an area of memory in a host that is directly accessible by a host application.

20.   (Currently Amended) A host for connection to a network, the host comprising:

a network analyser card for receiving data from the network;

a memory to receive at least two new replica editions of one or more frames of the received data from the network analyser card; and

at least two processors for processing said at least two new replica editions of the received data, wherein the network analyser card includes

4

a receiver for receiving plural data frames from the network;

data replication means for generating at least two replica editions of the received data frames; and

a descriptor adder configured and arranged to add a descriptor to substantially each of the data frames of each of the at least two replica editions of the received data frames, the descriptor including data about the data frame to which it is attached for use in processing of the data frame.

21.   (Previously Presented) The host according to claim 20, wherein each of the at least two processors is arranged to execute a different set of rules on each edition of the stored data.

22.   (Previously Presented) The host according to claim 21, wherein the rules relate to intrusion detection.

23.   (Previously Presented) The intrusion detection system, comprising a host according to claim 20, wherein the processors are arranged to execute rules of an intrusion detection system on data packets received by the host.

5